

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-5782

(P2001-5782A)

(43)公開日 平成13年1月12日 (2001.1.12)

(51)Int.Cl. ⁷	識別記号	F I	デマコト* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A
12/66		11/20	B

審査請求 未請求 請求項の数21 O L (全 8 頁)

(21)出願番号 特願2000-133828(P2000-133828)

(22)出願日 平成12年5月2日(2000.5.2)

(31)優先権主張番号 09/303424

(32)優先日 平成11年5月3日(1999.5.3)

(33)優先権主張国 米国 (US)

(71)出願人 591275137

ノキア モービル フォーンズ リミテ
ドNOKIA MOBILE PHONES
LIMITEDフィンランド 02150 エスプー ケイラ
ラーデンティエ 4

(72)発明者 ジュシー レミライネン

フィンランド タンペレ 33720 オリヴ
エデンカツ 16 シー 61

(74)代理人 100086368

弁理士 萩原 誠

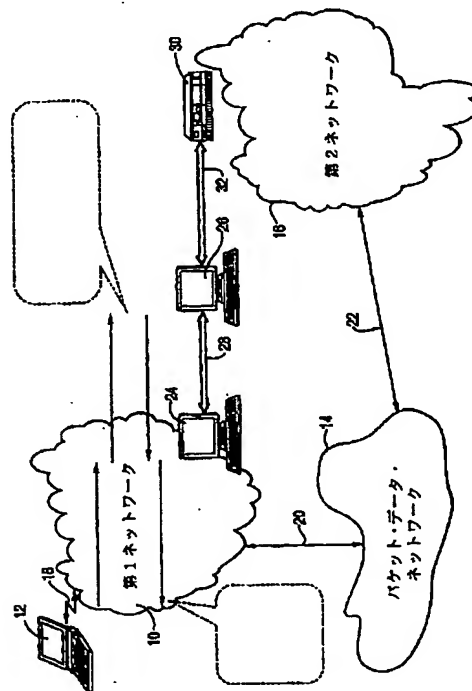
最終頁に続く

(54)【発明の名称】 公衆ISPアクセスネットワークにおける支払方法としてのSIMベースの認証方法と認証システム

(57)【要約】

【課題】 ユーザーのホームネットワークとローミング先ネットワークとの間に課金協定がなくても、ユーザーがローミング先でパケット・データ・ネットワークに接続することを可能とする方法を提供する。

【解決手段】 第2ネットワーク(16)を通しての該パケット・データ・ネットワーク(14)との接続をユーザー(12)に対して承諾するように要求するユーザー要求を第1ネットワーク(10)に入力し;該ユーザー要求と、該ユーザーによる該パケット・データ・ネットワークの利用についての該第1ネットワークによる該第2ネットワークへの支払いの承認とを該第1ネットワークから該第2ネットワークに送り;該第2ネットワークを通して該パケット・データ・ネットワークとの接続を得ることを該ユーザーに対して承認する認証情報を該第2ネットワークから該第1ネットワークに送り;該パケット・データ・ネットワークとの接続を得るための認証が得られていることを該ユーザーに知らせる該認証情報を該第1ネットワークから該ユーザーに送るステップを含む。



(2)

特開 2001-5782

1

【特許請求の範囲】

【請求項 1】 パケット・データ・ネットワークとの接続を得る方法であって、この方法は：第 2 ネットワークを通しての前記パケット・データ・ネットワークとの接続をユーザーに対して承諾するように要求するユーザー要求を第 1 ネットワークに入力し；前記ユーザー要求と、前記ユーザーによる前記パケット・データ・ネットワークの利用についての前記第 1 ネットワークによる前記第 2 ネットワークへの支払いの承認とを前記第 1 ネットワークから前記第 2 ネットワークに送り；前記第 2 ネットワークを通して前記パケット・データ・ネットワークとの接続を得ることを前記ユーザーに対して承認する認証情報を前記第 2 ネットワークから前記第 1 ネットワークに送り；前記パケット・データ・ネットワークとの接続を得るための認証が得られていることを前記ユーザーに知らせる前記認証情報を前記第 1 ネットワークから前記ユーザーに送るステップを含むことを特徴とする方法。

【請求項 2】 前記ユーザー要求は前記ユーザーが前記パケット・データ・ネットワークに要求する接続の数量表示を含んでいることを特徴とする請求項 1 に記載の方法。

【請求項 3】 前記数量表示は少なくとも 1 つのサービス・ユニットを含み、各サービス・ユニットは乱数で符号化されていることを特徴とする請求項 2 に記載の方法。

【請求項 4】 前記各サービス・ユニットは異なる乱数で符号化されることを特徴とする請求項 3 に記載の方法。

【請求項 5】 前記認証情報は、前記ユーザーと前記パケット・データ・ネットワークとの間の機密保護通信メッセージを作るために使用され得る共有されるキーを含むことを特徴とする請求項 1 に記載の方法。

【請求項 6】 前記認証情報は、 n 個のサービス・ユニットを含む加入者識別モジュール SIM であり、各サービス・ユニットは、各サービス・ユニットを一義的に特定する異なるランダム・アクセス数と、署名入り応答 RES と、前記共有キー Kc とを含むことを特徴とする請求項 5 に記載の方法。

【請求項 7】 前記認証情報は、前記ユーザーと前記パケット・データ・ネットワークとの間の機密保護通信メッセージを作るために使用され得る共有されるキーを含むことを特徴とする請求項 2 に記載の方法。

【請求項 8】 前記認証情報は、 n 個のサービス・ユニットを含む加入者識別モジュール SIM であり、各サービス・ユニットは、各サービス・ユニットを一義的に特定する異なるランダム・アクセス数と、署名入り応答 RES と、前記共有キー Kc とを含むことを特徴とする請求項 7 に記載の方法。

【請求項 9】 前記認証情報は、前記ユーザーと前記パ

2

ケット・データ・ネットワークとの間の機密保護通信メッセージを作るために使用され得る共有されるキーを含むことを特徴とする請求項 3 に記載の方法。

【請求項 10】 前記第 2 ネットワークは、サービス・ユニットの数を含み加入者識別モジュール SIM を計算し、各サービス・ユニットは、各サービス・ユニットを一義的に特定する異なるランダム・アクセス数と、署名入り応答と、前記共有キー Kc とを含むことを特徴とする請求項 5 に記載の方法。

【請求項 11】 前記認証情報は、前記ユーザーと前記パケット・データ・ネットワークとの間の機密保護通信メッセージを作るために使用され得る共有されるキーを含むことを特徴とする請求項 4 に記載の方法。

【請求項 12】 前記認証情報は、サービス・ユニットの数を含み加入者識別モジュール SIM であり、各サービスは、各サービス・ユニットを一義的に特定する異なるランダム・アクセス数と、署名入り応答と、前記共有キーとを含むことを特徴とする請求項 11 に記載の方法。

【請求項 13】 前記第 1 ネットワークへの前記ユーザー要求の入力、前記ユーザー要求及び支払い承認の前記第 2 ネットワークへの送信、並びに前記第 2 ネットワークから前記第 1 ネットワーク及び前記ユーザーへの前記認証情報の送信とは機密保護通信メッセージによることを特徴とする請求項 1 に記載の方法。

【請求項 14】 前記第 1 ネットワークへの前記ユーザー要求の入力、前記ユーザー要求及び支払い承認の前記第 2 ネットワークへの送信、並びに前記第 2 ネットワークから前記第 1 ネットワーク及び前記ユーザーへの前記認証情報の送信は機密保護通信メッセージによることを特徴とする請求項 2 に記載の方法。

【請求項 15】 前記第 1 ネットワークへの前記ユーザー要求の入力、前記ユーザー要求及び支払い承認の前記第 2 ネットワークへの送信、並びに前記第 2 ネットワークから前記第 1 ネットワーク及び前記ユーザーへの前記認証情報の送信は機密保護通信メッセージによることを特徴とする請求項 3 に記載の方法。

【請求項 16】 前記第 1 ネットワークへの前記ユーザー要求の入力、前記ユーザー要求及び支払い承認の前記第 2 ネットワークへの送信、並びに前記第 2 ネットワークから前記第 1 ネットワーク及び前記ユーザーへの前記認証情報の送信とは機密保護通信メッセージによることを特徴とする請求項 4 に記載の方法。

【請求項 17】 前記第 1 ネットワークへの前記ユーザー要求の入力、前記ユーザー要求及び支払い承認の前記第 2 ネットワークへの送信、並びに前記第 2 ネットワークから前記第 1 ネットワーク及び前記ユーザーへの前記認証情報の送信とは機密保護通信メッセージによることを特徴とする請求項 5 に記載の方法。

【請求項 18】 前記パケット・データ・ネットワーク

との接続を得るための承認が得られていることがユーザーに知らされた後、前記ユーザーは、乱数RANDと署名入り応答SRESとを含む少なくとも1つのサービス・ユニットについての少なくとも1つの消費要求を前記第2ネットワークに送信し；前記第2ネットワークは、前記ユーザーから受け取った少なくとも1つのサービス・ユニットについての各消費要求の乱数RAND及び署名入り応答SRESを、蓄積されている乱数RAND及び署名入り応答SRESと比較して、一致するものがあるか否か判定し；もし一致するものがあれば、前記第2ネットワークは前記ユーザーと前記パケット・データ・ネットワークとの間でデータ・パケットが前記第2ネットワークを通過することを許可することを特徴とする請求項3に記載の方法。

【請求項19】 前記第2ネットワークは、消費済みサービス・ユニットの数が承諾されたサービス・ユニットの数に等しくなるまで、前記ユーザーに対して承諾されているサービス・ユニットの蓄積されている値から、少なくとも1つのサービス・ユニットについての各消費要求で特定されている消費済みサービス・ユニットの数を借方に記入することを特徴とする請求項18に記載の方法。

【請求項20】 未使用の各サービス・ユニットは前記第2ネットワークにおいてハッシュ・テーブルに蓄積され、使用済みの各サービス・ユニットは前記第2ネットワークにおいてハッシュ・テーブルに蓄積されることを特徴とする請求項19に記載の方法。

【請求項21】 ユーザーと；前記ユーザーに接続することのできる第1ネットワークと；前記第1ネットワーク及び前記ユーザーに接続することのできる第2ネットワークと；前記第2ネットワークに接続することのできるパケット・データ・ネットワークとを含むシステムにおいて；前記第1ネットワークは、前記ユーザーが前記第2ネットワークを通して前記パケット・データ・ネットワークと接続するための承認を前記第1ネットワークに求めるユーザー要求に応じて、前記ユーザー要求と、前記パケット・データ・ネットワークの前記ユーザーによる利用についての前記第1ネットワークによる支払いの承認とを前記第2ネットワークに送り、前記第2ネットワークは、前記第2ネットワークを通して前記パケット・データ・ネットワークとの接続を得ることを認める認証を前記ユーザーに承諾する認証情報を前記第1ネットワークに送り、前記第1ネットワークは、前記パケット・データ・ネットワークとの接続を得るための認証が得られたことを前記ユーザーに知らせる認証情報を前記ユーザーに送ることを特徴とするシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、パケット・データ・ネットワークへのアクセスの入手についてユーザー

(クライアント)に課金する方法及びシステムに関する。

【0002】

【従来の技術】ユーザー（人、PC及び電話等の通信装置）は、通常、法人アクセスネットワーク或いは公衆インターネット・サービス・プロバイダ（ISP）から提供される接続により、IPネットワーク（インターネット）等のパケット・データ・ネットワークとのアクセスを得る。法人アクセスネットワーク又はISPから提供される接続は、ユーザーの口座又は会社の口座に料金請求される多数のサービス全部を提供する。それらのサービスは、ユーザーがローミング時にアクセスしたいと望む同じサービスである。場合によっては、例えばユーザーのホーム・ネットワークと、ユーザーがローミングして、それを通してパケット・データ・ネットワークと接続する無線ネットワークとの間にローミング協定が存在するときなど、ユーザーがローミングしているとき、全ての料金はそれぞれのネットワーク間のローミング協定により自動的に処理される。その結果として、第2ネットワークを通してのパケット・データ・ネットワークとのユーザーの接続の結果として生じる課金は、ユーザーと第1ネットワークとの課金契約を通してシームレスに処理される。

【0003】しかし、パケット・データ・ネットワークへのアクセスをユーザーに提供する無線ネットワークにおいては特にありふれている或る状況においては、或いはユーザーのホーム・ネットワークとユーザーがローミングしてそれを通してパケット・データ・ネットワークに接続するネットワークとの間にユーザーに課金するローミング協定が存在しないとき、典型的ユーザーは第2ネットワークに関して匿名のままであることを望むことがある。その様な状況では、代わりの課金協定を設けなければならない。

【0004】GSM (Global System for Mobile Communications: 移動通信用広域システム) 電話システムは、移動ユーザー・ユニットとネットワーク・サーバーとにおいて、ユーザーの認証を制御してネットワークへの無認可のアクセスを防止すると共にユーザー間の通信を暗号化するアルゴリズムを使用する。GSMシステムは、Mouly及びPautetの刊行物“移動通信のためのGSMシステム (The GSM System for Mobile Communications)” (著作権1992) で詳しく解説されている。この刊行物の全体を参照により本書に取り入れる。GSMネットワークにおける認証は、ユーザーの移動端末装置とネットワークとの両方による署名入り応答SRESの作成により実行され、それはユーザーの移動端末装置に特有の秘密識別子Kiと乱数RANDとの関数である。署名入り応答SRESは、加入者識別モジュール (SIM) において、SIM内のKiと、ネットワーク認証センター (AUC) から入手されたRANDとに基づいて

5

計算される。また、ユーザーの移動端末装置とネットワークとは、各々、暗号化キーKcを作成することにより暗号化を行い、該キーは同じ乱数RANDと該ユーザー移動端末装置の秘密識別子Kiとの関数である。SRESを計算する第1認証アルゴリズムは、A3アルゴリズムとして知られており、ユーザーの移動端末装置が認証される毎に計算されるKcを計算する第2アルゴリズムはA8アルゴリズムとして知られている。しかし、認証と、暗号化キーKcの計算との動作の各々は、前述の計算を実行するように移動端末装置がプログラムされていることを必要とする。

【0005】

【課題を解決するための手段】本発明は、第2ネットワークを通してのIPネットワーク等のパケット・データ・ネットワークとのユーザーの接続についての、ユーザーを代理する第1ネットワークによる第2ネットワークへの支払いの方法及びシステムを提供する。本発明は、ユーザーと、該ユーザーによる第1ネットワークを通しての通信に課金するネットワークのセキュリティ・サーバーと、公衆セキュリティ・サーバーと、ユーザーとパケット・データ・ネットワークとの接続を与える第2ネットワークとの間の一連の通信メッセージを利用する。その一連の通信メッセージはユーザーがユーザー要求を第1ネットワークに入力する購入通信メッセージであり、そのメッセージは、指定された量の通信メッセージのために第2ネットワークを通じてユーザーがパケット・データ・ネットワークと接続できるように認可を要求するものであり、該通信メッセージを以降は“サービス・ユニット”と称する。サービス・ユニットは、無制限に、ユーザーの、第2ネットワークを通じてのパケット・データ・ネットワークとの指定された時間の接続を表わし、或いは、一定額の金銭に対して、サービス・ユニットは接続の時間又はその他の要素に左右される料金構造に応じて変化する量のパケット・データ・ネットワークとの接続時間を提供する。ユーザーのホーム・セキュリティ・サーバーは、第2ネットワークの公衆セキュリティ・サーバーにユーザー要求と、第2ネットワークを通じてのユーザーによるパケット・データ・ネットワークの利用についての第1ネットワークによる第2ネットワークへの支払いの認証とを送る。その後、第2ネットワークは、第2ネットワークを通じてパケット・データ・ネットワークとの接続を得るためのユーザー認証を承諾する認証情報を第1ネットワークに送る。第2ネットワークによる認証情報の計算は、GSMシステムにおけるSIMと似ている計算を実行する常駐SIMによって実行される。認証情報は第1ネットワークからユーザーに送られ、情報は、パケット・データ・ネットワークとの接続を得るための認証が得られたことをユーザーに知らせる。ユーザー要求は、パケット・データ・ネットワークとのユーザーの接続の数量表示を含んでおり、その

6

数量表示は少なくとも1つのサービス・ユニットから成り、各々のサービス・ユニットは乱数で符号化されている。好ましくは、各サービス・ユニットは、異なる乱数で符号化される。認証情報は、更に、ユーザーとパケット・データ・ネットワークとの間の機密保護通信メッセージを作るのに使われる共有されるキーを含む。認証情報は、加入者識別モジュールSIMにより計算され、数個(n個)のサービス・ユニットを包含し、各々のサービス・ユニットは、各サービス・ユニットを一義的に特定する異なるランダム・アクセス数と、署名入り応答と、共有キーとを含む。

【0006】好ましくは、第1ネットワークへのユーザー要求の入力、第2ネットワークへのユーザー要求及び支払い認証の送信、並びに第2ネットワークから第1ネットワーク及びユーザーへの認証情報の送信は、秘密通信による。従って、共有される秘密キーKcの送信は公開されず、従って、GSM通信の場合のようにユーザーとパケット・データ・ネットワークとの後の通信の際にユーザーとパケット・データ・ネットワークとの間に秘密通信を確立するために共有秘密キーKcを計算するアルゴリズムをユーザー端末装置が内蔵していなくても良い。

【0007】パケット・データ・ネットワークへのアクセスが承認され、例えば(それに限らないけれども)ローミング中にパケット・データ・ネットワークへのアクセスが認可され、ユーザーが第2ネットワークへの送信を開始することによってアクセスが開始されたことがユーザーに知らされた後に、承認されたサービス・ユニットの消費が始まり、少なくとも1つのサービス・ユニットの消費についての少なくとも1つの要求は、乱数と署名入り応答とを含む。第2ネットワークは、ユーザーから受け取った少なくとも1つのサービス・ユニットの消費についての各要求の乱数及び署名入り応答を、蓄積されている乱数及び署名入り応答と比較して、一致するかどうか確かめる。もし一致するものがあれば、第2ネットワークはデータ・パケットがユーザーとパケット・データ・ネットワークとの間で第2ネットワークを通過することを許す。第2ネットワークは、消費されたサービス・ユニットの数が承諾されたサービス・ユニットの数nと等しくなるまで、ユーザーに対して承諾されたサービス・ユニットの蓄積されている値nから、少なくとも1つのサービス・ユニットについての各消費要求で特定されている消費済みサービス・ユニットの数を借方に記入する。好ましいアプリケーションでは、未使用の各サービス・ユニットは第2ネットワークにおいて第1リストに蓄積され、各使用済みサービス・ユニットは第2ネットワークにおいて第2リストに蓄積される。好ましくは、その第1及び第2のリストは、サービス・ユニットの、起こる可能性のある衝突を防止するハッシュ・テーブルである。

7

【0008】本発明のシステムは、ユーザーと；ユーザーと接続できる第1ネットワークと；第1ネットワーク及びユーザーと接続できる第2ネットワークと；第2ネットワークと接続できるパケット・データ・ネットワークとを包含しており；第1ネットワークは、ユーザーが第2ネットワークを通してパケット・データ・ネットワークと接続するための承認を第1ネットワークに求めるユーザー要求に応じて、ユーザー要求と、パケット・データ・ネットワークのユーザーによる利用についての第1ネットワークによる支払いの承認とを第2ネットワークに送り、第2ネットワークは、第2ネットワークを通してパケット・データ・ネットワークとの接続を得ることを認める認証をユーザーに承諾する認証情報を第1ネットワークに送り、第1ネットワークは、パケット・データ・ネットワークとの接続を得るための認証が得られたことをユーザーに知らせる認証情報をユーザーに送る。

【0009】全図にわたって、同様の部分を特定するために同様の参照数字及び用語が使われている。

【0010】

【発明の実施の形態】図1は、第2ネットワーク16を通してパケット・データ・ネットワーク14とのユーザー12（例えばコンピュータ及びモデム）の接続を提供するために第1ネットワーク10によりユーザー12に料金請求されるサービス・ユニット購入の図を示している。その購入についての料金請求は、第1ネットワーク10からユーザー12に対して行われる。購入されるのは、第2ネットワーク16経由でのユーザーによるパケット・データ・ネットワーク14との接続のnサービス・ユニットであり、それは第2ネットワーク16を通しての

パケット・データ・ネットワークとのユーザーの接続により消費される。第2ネットワークは、単一のエンティティとは限らず、種々の技術で実現され得る複数の地理的に離れているアクセスネットワークから構成されていても良いことが理解されなければならない。第2ネットワークは、ユーザー12がそれを通してパケット・データ・ネットワーク14との接続を得る如何なる種類のネットワークであっても良い。図示されているように、第1ネットワークとのユーザー12の接続は、例えばセルラー、PCS、802.11、無線LANなど（これらに限定はされない）の任意の種類の無線サービスにより提供される無線リンク18を経由しているけれども、第1ネットワーク10との、ワイヤーラインを含むあらゆる種類の接続が本発明の範囲内にあることが理解されなければならない。図示されている通信ライン20経由でのパケット・データ・ネットワーク14とのユーザー12の接続は、在来のものであり、本発明の一部ではない。購入されたnサービス・ユニット（nは任意の整数である）は、後に図2に示されているように

（後述するように）ユーザーが第2ネットワーク16を

8

通してパケット・データ・ネットワーク14にアクセスするときに認証とユーザー12への料金請求とのために使用される。

【0011】最初の購入シーケンスは、図1に示されているようにnサービス・ユニットを購入するための4ステップを含んでいる。第1ステップ“1”は、第1ネットワーク10のホーム・セキュリティ・サーバー24に送られる、nサービス・ユニットの購入を求めるユーザー要求をユーザー12がユーザーのプロセッサから入力することを含む。nサービス・ユニットの購入は、アクセスを提供すると共に、第2ネットワーク16を通しての

パケット・データ・ネットワーク14との通信の量又は値を指定する。購入されたn個のサービス・ユニットは第2ネットワーク16を通してパケット・データ・ネットワーク14と接続するための権限をユーザーに与える第1ネットワーク10のホーム・セキュリティ・サーバー24に送られ、第2ネットワーク16は、好ましいアプリケーションでは、ユーザー12がローミングしているときにパケット・データ・ネットワークとの接続を提供する。

【0012】第2ステップは、ホーム・セキュリティ・サーバー24と第2ネットワーク16の公衆セキュリティ・サーバー26との間での送信“2”であり、それは各サービス・ユニットに独特の識別乱数RANDを割り当てることによってn個のサービス・ユニットを数量表示する。或いは、独特の各ランドは、ユーザー12によって作られてnサービス・ユニットの一部分としてホーム・セキュリティ・サーバー24に回送されても良い。

【0013】ホーム・セキュリティ・サーバー24と公衆セキュリティ・サーバー26との間での通信は、機密保護リンク28を介して行われる。第2ネットワーク16のアクセスサーバー30は、機密保護通信リンク32により公衆セキュリティ・サーバー26に接続される。アクセスサーバー30は、公衆セキュリティ・サーバー26と共同して、図2との関連で後述するように、機密保護されない通信リンク22を経由する第2ネットワーク16とパケット・データ・ネットワーク14との間でのパケットの通行を制御する。好ましくは、リンク18経由でのホーム・セキュリティ・サーバー24へのユーザー要求と、ホーム・セキュリティ・サーバー及び公衆セキュリティ・サーバー26の間での、第2ネットワーク16から購入されるべきnサービス・ユニットを特定するn個の乱数の伝送とは機密保護リンクを介して行われる。各々独特の乱数RANDとして個別に符号化されるのが好ましいnサービス・ユニットの数量表示にくわえて、ホーム・セキュリティ・サーバー24と公衆セキュリティ・サーバー26との間での第2伝送“2”は、支払い（電子支払い（Eキャッシュ））によるのが好ましい）の授權を含んでいる。しかし、ユーザーのパケット・データ・ネットワーク14との接続を確保するために

第1ネットワーク10から第2ネットワーク16への支払いを清算する任意のメカニズムであって良い。

【0014】公衆セキュリティ・サーバー26は、nサービス・ユニットを計算して、それを第1リストに蓄積するが、該第1リストは未使用のサービス・ユニットの個数を蓄積するハッシュ・テーブルであるのが好ましい。更に、ハッシュ・テーブルであるのが好ましいかも知れない第2リストは、n個の承認されたサービス・ユニットから消費されたサービス・ユニットを明らかにする。或いは、サービス・ユニットが消費されたら直ちにその消費済みサービス・ユニットを削除することによって第2リストを無くしても良い。ハッシュ・テーブルは、周知のハッシング関数（周知なので、これについては詳しく説明はしない）に依拠するものであり、n個の承認されているサービス・ユニット全部の場所を、その承認から消費に至る過程で、見つけたための独特のアドレスを提供する。消費段階において、図2に関して後述するように、ユーザー12のケット・データ・ネットワーク14との購入された量（時間又は金額）の接続だけが生じることを保証するために、未使用サービス・ユニットと使用済みサービス・ユニットとが明らかにされる。

【0015】購入段階の第3ステップは、個々のサービス・ユニットを符号化するのに必要な情報に各々対応するn情報トリプレットの形の認証情報の、第2ネットワーク16の公衆セキュリティ・サーバー26から第1ネットワークへの送信“3”である。該認証情報は、好ましくは、各サービス・ユニットについて、個々の乱数RANDと、従来技術のA3アルゴリズムを用いてGSM認証により計算される署名入り応答と同様に計算される署名入り応答SRESと、第2ネットワーク16を通してのユーザー12とケット・データ・ネットワーク14との間での機密保護通信を提供するために使うことのできる暗号化キーKcとを含む。暗号化キーKcは、図2の消費段階におけるアクセスサーバー30とユーザー12との間で共有されるキーでもある。

【0016】購入段階の第4ステップは送信“4”であり、その間に、ホーム・セキュリティ・サーバー24は、RAND、SRES、Kcのnトリプレットから成る認証情報を受け取り、データネットワーク14における消費のためのサービス・ユニットの購入が完了していることをユーザーに知らせるそのnトリプレットをユーザー12に回送する。この第4段階で購入シーケンスは完了し、これでユーザー12は、第2ネットワーク16を通してのケット・データ・ネットワーク14との一定時間単位の接続、又は、時間（ゴールデンアワー及びオフタイム）又はその他の基準の関数として変化する接続を表わす可変数のサービス・ユニットを確保することができる。

【0017】ユーザー12が認証情報を受け取るとき、

ユーザー及び公衆セキュリティ・サーバー26は、nサービス・ユニットの消費時に第2ネットワーク16を通じてユーザーとケット・データ・ネットワーク14との秘密通信を確立するのに必要な共有暗号化キーKcを記憶装置に有することに留意することが重要である。公衆セキュリティ・サーバー26による署名入り応答SRES及び共有秘密暗号化キーKcの作成並びに秘密通信リンク28を介して、それをホーム・セキュリティ・サーバー24に送信し、且つ、ホーム・セキュリティ・サーバー24からユーザー12に送信することは、秘密通信及び/又はユーザー認証を行うのに必要な共有暗号化キーKcの初期計算の原因が公衆セキュリティ・サーバー26であることを考慮すると、ユーザーのプロセッサがサービス・ユニットを購入して消費するのにA3及びA8アルゴリズム（これらはGSM認証で利用される）が存在することをサービス・ユニットの購入が必要とするという必要条件を無くする。

【0018】本発明の方法の第2消費段階は、図2に示されている3つのステップを含んでいる。図示されているように、ユーザー12は、ローミングし（第1ネットワーク10との接続から移行している）、リンク18'（これは無線リンクであるのが好ましいけれども、本発明はそれに限定はされないことが理解されなければならない）を介して第2ネットワーク16にアクセスする。アクセスサーバー30は、第2ネットワーク16へのユーザーのアクセスと、随意に、nサービス・ユニットの消費時にユーザー12とケット・データ・ネットワーク14との間でのデータ・ケットの交通とを制御する。しかし、アクセスサーバーはユーザー12が新たに第2ネットワークと接続するときに認証を行うだけでも良く、その後、アクセスサーバーは、ユーザーが第2ネットワークに接続している間、ユーザーとデータ・ケット14との間でのデータ交換に全く関わらなくても良い。

【0019】第1ステップは、ケット・データ・ネットワーク14との接続についての承認が得られていることがユーザーに知らされた後、ユーザー12が少なくとも1つのアクセス要求を含む第1通信メッセージ“1”を第2ネットワーク16のアクセスサーバー30にリンク18'を介して送ることを必要とする。各アクセス要求は、各サービス・ユニットの識別情報を構成する個別の乱数RAND及び署名入り応答SRESを含んでいる。

【0020】第2ステップは、アクセスサーバー30から公衆セキュリティ・サーバー26に中継されるアクセス要求である通信メッセージ“2”を含む。公衆セキュリティ・サーバー26は、ユーザー12から受け取った少なくとも1のサービス・ユニットの消費を求める各要求の各乱数RAND及び署名入り応答SRESを、公衆セキュリティ・サーバーに蓄積されている乱数RAND

及び署名入り応答SRESと比較して一致するものがあるか否か判定する。一致するものが存在することを公衆セキュリティ・サーバー26が発見すると、第2ネットワーク16のアクセスサーバー30は通信メッセージのデータ・パケットがユーザー12とパケット・データ・ネットワーク14との間で第2ネットワークを通過することを許す。

【0021】第2ネットワーク16の公衆セキュリティ・サーバー26は、消費済みサービス・ユニットの数が承諾されたサービス・ユニットの数nに等しくなるまで、第1ネットワーク10と第2ネットワーク16との間で支払条件に達した結果としてユーザー12に対して承諾された、第1リスト或いはハッシュ・テーブルに蓄積されているサービス・ユニットの値nから、少なくとも1つのサービス・ユニットについての各消費要求で特定されている消費済みサービス・ユニットの数を借方に記入する。第2の随意リスト又はハッシュ・テーブルは、公衆セキュリティ・サーバー26に戻されて消費されたと確認されたサービス・ユニットを蓄積する。従って、承諾されたサービス・ユニットと、消費されたサービス・ユニットと、消費されていないサービス・ユニットとについての合計額が公衆セキュリティ・サーバー26において常時維持され、或いは、もし第2リストが使われないのであれば、未消費サービス・ユニットの第1リストだけが維持され、消費済みサービス・ユニットはそれから削除される。公衆セキュリティ・サーバー26が各サービス・ユニットと一致するものを見つけると、各サービス・ユニットの乱数RAND及び署名入り応答SRESに基づいて該リストから暗号化キーKcが計算される。

【0022】第3ステップは、ユーザー12とパケット・データ・ネットワーク14とが第2ネットワーク16を通して通信することを許可するアクセス承諾である通信メッセージ“3”である。ユーザー12に対して承諾された、第2ネットワーク16とパケット・データ・ネットワークとの間の機密保護されない通信路22を通してのパケット・データ・ネットワーク14へのアクセス

を暗号化するために暗号化キーKcが使われる。一方、公衆セキュリティ・サーバー26に受け取られたサービス・ユニットと、蓄積されているサービス・ユニットとの一致が得られなかったならば、アクセスサーバー30は、機密保護されない通信路22を介してのユーザー12とパケット・データ・ネットワーク14との接続を拒否する。

【0023】本発明は、前述したネットワーク・アーキテクチャには限定されなくて、いろいろなネットワーク構成で実施され得るということが理解されなければならない。更に、本発明が実施されるネットワークのデザインは周知されていて、それ自体は本発明の一部ではない。また、図1及び2の購入及び消費の方法の際にユーザー12と第1ネットワーク10と第2ネットワーク16との間の通信メッセージを符号化するために使われる方法は、本発明の一部ではないいろいろな方法で達成され得る。

【0024】本発明をその好ましい実施態様に関して説明したけれども、添付の請求項で定義されている本発明の範囲から逸脱することなく、それに数々の修正を加え得ることが理解されなければならない。その様な修正は全て添付の請求項の範囲に属する。

【図面の簡単な説明】

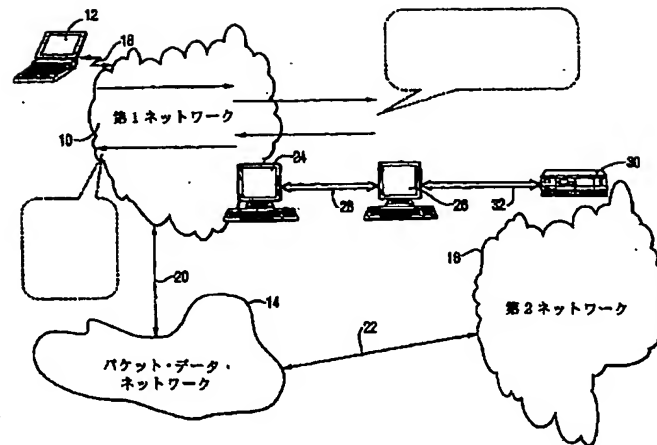
【図1】第2ネットワークを通してパケット・データ・ネットワークとの接続を提供する第1ネットワークでユーザーが本発明に従ってサービス・ユニットを購入する方法を示している。

【図2】第2ネットワークを通してパケット・データ・ネットワークに接続している間に、図1に示されている方法によって得られた購入されたサービス・ユニットのユーザーによる消費を示している。

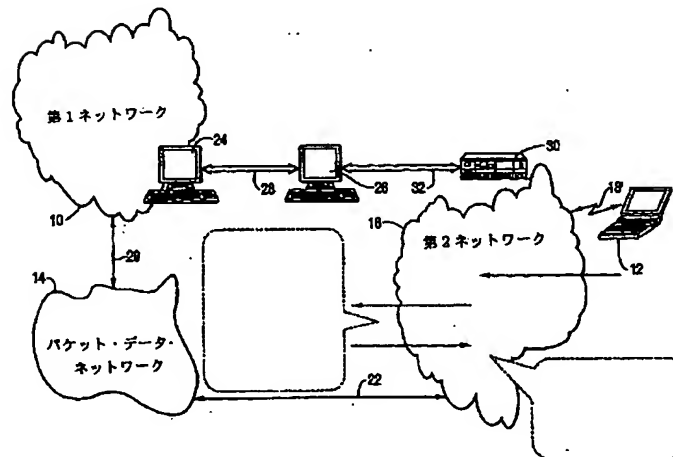
【符号の説明】

- 10 第1ネットワーク
- 12 ユーザー
- 14 パケット・データ・ネットワーク
- 16 第2ネットワーク

【図1】



【図2】



フロントページの続き

(72)発明者 ジャーンーエリック エコベルグ
 フィンランド ヘルシンキ 00320 セル
 ジャティエ 1 エー 5